بسم الله الرحمن الرحيم

الحمدلله رب العالمين والصلاة والسلام على أشرف المرسلين محمد وعلى آله وصحبه أجمعين

اليوم بعون الله سأطرح بعض الأفكار والنصائح لحماية نفسك أثناء الاتصال بشبكة الانترنت وحماية حسابات التويتر من المتطفلين

نبدأ على بركة الله

قبل أن تقوم بإنشاء حساب تويتر فبالطبع أنت ستحتاج إلى أمرين مهمين

- بريد إلكتروني
- إتصال إنترنت آمن

سنبني على هذين الامرين عده نصائح أمنية مهمة يجب إتباعها

البريد الإلكتروني

١. يجب الحصول على بريد إلكتروني آمن ومشفر ومن مزود خدمة لاينتهك خصوصية مشتركية ولايقوم بتتبعهم ويملك خيارات واساليب أمان عاليه

.

أمثله لخدمات مشفرة وآمنة (hushmail.com - tutanota.de)

٢. لابد من ضبط خيارات الأمان للبريد الإلكتروني بحيث يكون بكلمة سرية معقده تحتوي على أحرف كبيرة وأحرف صغيرة وأرقام ورموز ولم يسبق لك إستخدام نفس كلمة المرور في أي موقع أو خدمه أخرى (كلمة مرور جديدة وخاصة)

٣. ضبط سؤال سري لخيارات إستعادة البريد بحيث لايمكن تخمينها ويفضل أن تكون الاجابه منافيه للسؤال أو غير منطقية
مثال (أول سيارة إمتلكتها -> يكون الجواب مثلاً iNu٠٨@o) على أن تكون متذكراً لهذه الإجابه .

٤. لايفضل وضع إيميل بديل كـ Hotmail أو gmail في خيارات الإستعادة .

٥. بعد تسجيل البريد لاينبغي أن يكون معلوماً لدى أحد ولاينبغي أن يحمل نفس يوزر حسابك في تويتر فمن الخطأ أن يكون حسابك في تويتر مثلاً user١@ وتقوم بربطه ببريد user١@tutanota.de فبهذه الحالة أنت تسهل على من يستهدفك تخمين بريدك الإلكتروني وجمع المعلومات عنك .

٦. بريدك هذا لاتستخدمه نهائياً في أي مواقع أخرى ولاتتصفحه أبداً إلا عند الحاجة لإعادة تعيين كلمة المرور للحساب في حال نسيانها .

٧. تسجيل البريد + تصفحه يتم من خلال الإتصال الآمن وسيتم التطرق له في النقطة التالية .

الإتصال الآمن بالإنترنت

أي عملية إتصال بالانترنت لابد أن يكون لها أدوات ومايهمنا نحن هنا هو أمرين فقط :

- النظام المستخدم للإتصال
- طريقة حماية الإتصال وتجاوز الرقابه

١.النظام:

في عصرنا الحالي تعددت الأنظمة المستخدمه من قبل العامة وأكثرها شيوعاً Microsoft + Linux + Android + IOS

ولإستخدام هذه الأنظمة بشكل آمن لابد من تهيئتها وضبطها لتحافظ على خصوصيتك ولتكون جاهزة لصد أي هجمات قد تستهدفها لذلك سنتحدث عن عدة نقاط تخدم فكرة أمان النظام وحماية خصوصيته .

((التشفير))

هي عملية تعمية البيانات وعند تفعيله على نظامك فأنت تجعله يقوم بإعادة كتابة بياناتك الحالية أو المستقبلية بطريقة مشفرة بحيث تجعل أي بيانات مسروقة منك غير مفهومة وعديمة الفائدة وتعتبر هذه العملية أكبر عائق أمام المتطفل حتى ولو إستطاع سرقة جهازك أو مصادرته .

...

- التشفير في نظام Windows

أفضل أدوات التشفير لهذا النظام هو VeraCrypt

التحميل | شرح فيديو

أو إستخدام خاصية التشفير المدمجه مع غالب أنظمة windows وهي Bitlocker

شرح فيديو

...

- التشفير في نظام Android

خاصية التشفير في هذا النظام تأتي مدمجه معه وإختيارية

شرح فيديو

...

- التشفير في أنظمة أبل

IOS :

شرح فيديو

Mac OS :

شرح فيديو

...

((حماية النظام من أدوات التجسس والفيروسات))

بعد عملية التشفير الكامل للنظام يبقى الخطوة الاهم وهي حماية النظام من الفيروسات وتروجانات الإختراق

فمع التطور المستمر في عالم التجسس والإختراق لم يعد برنامج حماية واحد كافٍ لتأمين الحماية فأصبح لزاماً إختيار مجموعه من الأدوات التي لا تتعارض مع بعضها لتحقيق أكبر قدر ممكن من الأمان لجهازك .

حماية نظام Windows

يفضل إستخدام البرامج التالية مجتمعه :

- **Kaspersky للحماية من الفيروسات آخر إصدار أو Avast آخر إصدار .**
- **Malwarebytes Anti-Exploit للحماية من ثغرات التصفح .**
- **Total Security ٣٦٠ مكافح الفيروسات .**
- **Zemana AntiLogger لحماية بياناتك التي تتناقلها من خلال الكيببورد ومن خلال الكاميرا او المايك .**

حماية أنظمة الهواتف الذكية

- **Kaspersky Mobile أو Avast Mobile مع الإهتمام بالتحديث المستمر.**
- **Malwarebytes Anti-Malware لأجهزة أندرويد .**

- أجهزة Android يفضل إستخدام رومات cyanogenmod مع تفعيل خاصية Privacy Guard لضبط صلاحية التطبيقات (شرح فيديو)
- بخصوص الايفون فهو نظام مشفر ويدعي مطوروه انه محمي ولايوجد له برامج حماية أثبتت وجودها .

٢. حماية الإتصال بالإنترنت :

طرق حماية الاتصال وتعميته أثناء الاتصال بشبكة الإنترنت كثيرة ومعقدة وغالبها ليس مع خصوصية مستخدميه ولايخدم أهدافهم عوضاً أن بعض هذه الخدمات تعود إلى جهات إستخباراتية والبعض منها يعود إلى جهات ربحية تستغل مستخدميها في جني الأرباح منها تقنية Proxy ومنها تقنيات الـ VPN ومنها مايعتمد على الاثنين مجتمعه وعلى خوادم خاصة OpenVpn

في هذه الجزئية سنتحدث عن الفكرة الأكثر أماناً والأكثر موثوقية ألا وهي تقنية Tor

هذه الخدمة يسعى مطوروها والعاملين عليها على إخفاء نشاطات مستخدميها عبر الشبكة وتعميتها وحمايتهم من تتبع الجواسيس والمتطفلين ، تتم بتشفير عمليات الاتصال من وإلى شبكة الإنترنت وتمريرها على مجموعه خوادم تجعل من الصعب تعقب صاحب الإتصال

Tor Project

التثبيت على windows | التثبيت على Android | التثبيت على IOS

نصائح مهمة لحماية حساب تويتر

١. لاتقم بتصفح تويتر إلا من خلال الـ Tor أو على أقل تقدير VPN مأمون كـ avastsecure فتويتر مؤخراً أصبح يقوم بحفظ بيانات رقم الـ IP الخاصة بكل مستخدم فلولا قدر الله تمكن احدهم من الدخول إلى حسابك فسيكون العثور عليك أمر سهل من خلال هذا الرقم ولكن مع Tor فأنت تتصفح من خلال IP ليس حقيقي .

٢. لاتقم بحفظ رسائلك الخاصة لفترة طويلة فبمجرد إنتهائك من المراسلة لابد من حذف المحادثات .

٣. إحذر من الروابط المنتشرة في الهاشتاقات ولاتحاول فتح أي روابط مشبوهة تصلك عبر الخاص أو من خلال البريد الالكتروني كالتي تطلب منك إعادة تعيين كلمة المرور أو التي تطلب منك تسجيل الدخول أو تحميل ملفات على جهازك .

٤. تعامل مع الجميع على أنهم جواسيس وإنسى مبدا الثقة حتى لو من أقرب صديق فلا تعلم فربما يتم إختراق حساب هذا الصديق ويتم إستدراجك من خلاله .

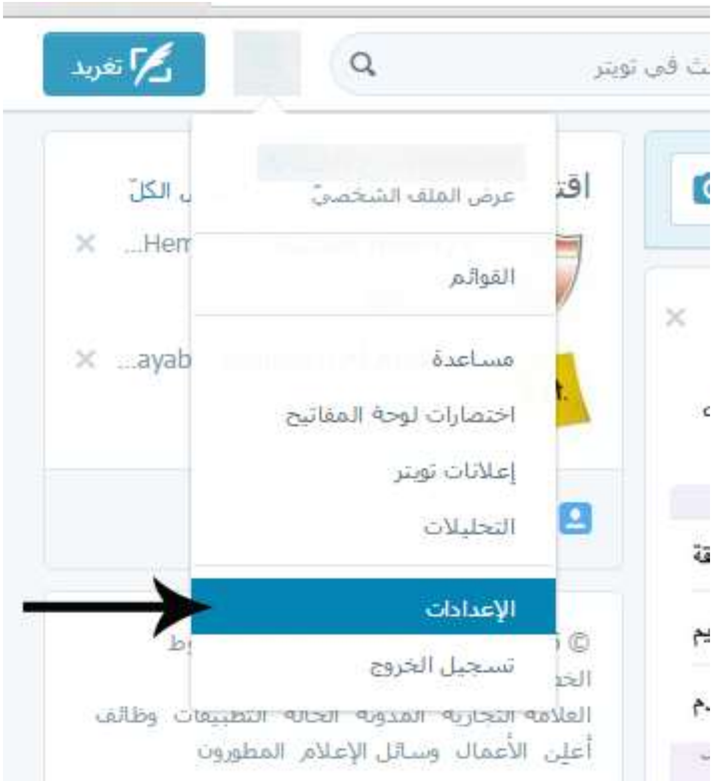
٥. لاتقم بأي حال من الأحوال بالإشتراك في أي تطبيق خاص سواء للأذكار أو غير ذلك فأغلب هذه التطبيقات تملك صلاحيات للتحكم بحسابك لاينبغي أن تمتلكها كما أن اصحابها غير معروفين ولايؤمن جانبهم وحتى إن أمن جانبهم فلو تم إختراق موقع أحد هذه التطبيقات أو أخترق الحساب المؤسس للتطبيق فستصبح حسابات جميع المستخدمين المشتركين فيه عرضة للخطر .

٦. في حال شعرت بمحاولة لإختراق حسابك سواء بوصول رساله لإستعادة كلمة المرور أو ظهور رساله من تويتر تبلغك أن هناك من يحاول الدخول

إلى حسـابك بـادر مباشـرة بتغيير باسـورد الحسـاب + يـوزر الحسـاب + تسجيل إيميل جديد بباسورد جديد وربطه بالحساب مباشرة .

<u>أمور لابد من تفعيلها بحسابك على تويتر</u>

- قم بتصفح حسابك من خلال الحاسوب وإذهب إلى الإعدادات



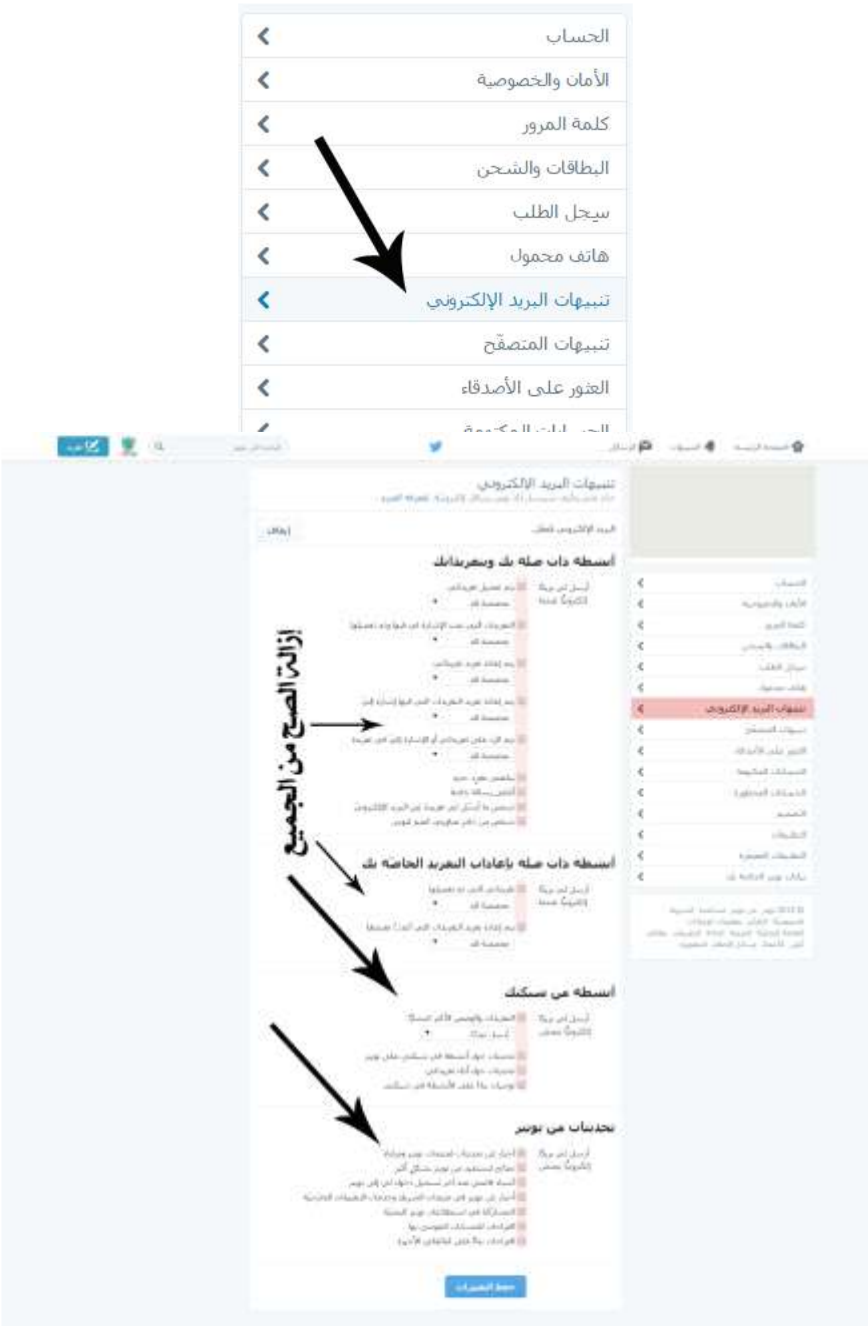
- قم بالدخول على الأمان والخصوصية



- قم بضبط الاعدادات كما هو موضح بالصورة تماماً مع التركيز على المعلم بأسهم



ثم إنتقل إلى تنبيهات البريد الإلكتروني وإضبط الاعدادات كما بالصورة



هذا ماتيسر طرحه

من أخيكم

إرشادات تقنية

@4UrIn

والحمدلله رب العالمين